Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for presentation integrity, comprising:

an encrypter embodied in a data processing device to encrypt formatting data associated with information content data; and

a formatter embodied in another data processing device associated with one of each of a plurality of different requesters or clients to decrypt the encrypted formatting data and to format the information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at each of the plurality of different requesters or clients caused by at least one of different types of browsers being used by at least some of the plurality of different requesters or clients, different types of browser settings being used by at least some of the plurality of different requesters or clients, different types of display settings being used by at least some of the plurality of different requesters or clients, and insecurity of a communications network, channel or medium, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each of the plurality of requesters or clients ~~requester or client~~ to provide presentation integrity between the different requesters or clients despite differences in browsers, browser settings and display settings of at least some of the plurality of different requesters or clients and despite insecurity of the communications network, channel or medium, and wherein the plurality of different requesters or clients are involved in a situation together requiring presentation integrity to prevent any confusion, misunderstanding, delays in coordination or other adverse effects between each of the plurality of different requesters or clients involved in the situation.

2. (Original) The system of claim 1, further comprising a plurality of formatters, each to decrypt the encrypted formatting data and to format the information content data in the predetermined format based on the decrypted formatting data.

3. (Previously Presented) The system of claim 1, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

4. (Original) The system of claim 1, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assigned to a different copy of the information content data.

5. (Original) The system of claim 1, further comprising an output device to present the information content data in the predetermined format.

6. (Original) The system of claim 5, wherein the output device comprises at least one of a display and a printer.

7. (Original) The system of claim 1, further comprising at least one of a computer and a media player to present the information content data in the predetermined format, wherein the formatter is embodied in the at least one of the computer or the media player.

8. (Cancelled)

9. (Previously Presented) The system of claim 1, wherein the formatting data is encryptable and decryptable by a common key.

10. (Previously Presented) The system of claim 1, wherein the formatting data is encryptable and decryptable by different keys.

11. (Original) The system of claim 1, wherein the information content data is encryptable by the encrypter.

12. (Original) The system of claim 11, wherein the information content data and the formatting data are decryptable in response to a valid key.

13. (Original) The system of claim 11, wherein the information content data and the formatting data are each decryptable in response to different keys.

14. (Original) The system of claim 11, wherein the information content data and the formatting data are encryptable in response to different keys and are decryptable in response to keys that are each different from the keys used to respectively encrypt the information content data and the formatting data.

15. (Original) The system of claim 1, wherein the encrypter encrypts the formatting data into an encrypted style sheet language transformation (SLT).

16. (Original) The system of claim 15, wherein the SLT is an extensible style language transformation (XSLT).

17. (Original) The system of claim 15, wherein the formatter decrypts the encrypted SLT and transforms the information content data into a hypertext markup language (HTML) having the predetermined format in response to a valid password.

18. (Original) The system of claim 17, further comprising a browser to receive the information content data in HTML and to present the information content data in the predetermined format.

19. (Original) The system of claim 1, wherein the encrypter encrypts the information content data into an encrypted markup language (ML) and encrypts the formatting data into an encrypted style sheet transformation (SLT).

20. (Original) The system of claim 19, further comprising an information broker to transmit the information content data in the encrypted ML and the formatting data in the encrypted SLT to the formatter, wherein the formatter transforms the encrypted ML into an HTML format based on the SLT in response to the formatter receiving a valid password.

21. (Currently Amended) A system for presentation integrity, comprising:

a formatter embodied in a data processing device to decrypt encrypted formatting data associated with information content data and to format the information content data into a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at a plurality of different requesters or clients, and wherein the formatting data is decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each of the plurality of different requesters or clients ~~information requester or client~~ to provide presentation integrity between the different requesters or clients, and wherein the plurality of different requesters or clients are involved in a situation together requiring presentation integrity to prevent any confusion, misunderstanding, delays in coordination or other adverse effects between each of the plurality of different requesters or clients involved in the situation; and

a device to present the information content data in the predetermined format.

22. (Original) The system of claim 21, further comprising a plurality of formatters, each to decrypt the encrypted formatting data and to format thc information content data in the predetermined format based on the decrypted formatting data.

23. (Original) The system of claim 21, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter.

24. (Previously Presented) The system of claim 23, wherein each predetermined format provides a different version of the information content data for presentation, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

25. (Original) The system of claim 23, wherein the information content data is presentable in different versions of the information content for different audiences, wherein the information content comprises onc of an audio, visual or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual or combination audio-visual work.

26. (Original) The system of claim 21, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid kcy being assignable to a different copy of the information content data.

27. (Original) The system of claim 21, further comprising at least one of a computer and a media player to form the information content data in the predetermined format, whcrein the formatter is embodied in the at least one of the computer or the media player.

28. (Original) The system of claim 21, wherein the formatter is adapted to be included in a vehicle.

29. (Original) The system of claim 28, wherein the vehicle comprises one of an aerospace vehicle, a watercraft and a terrestrial vehicle.

30. (Original) The system of claim 21, further comprising at least one of an aerospace communication channel and a terrestrial communication channel, wherein the formatter receives information content data and encrypted formatting data via at least one of the aerospace communication channel and the terrestrial communication channel.

31. (Original) The system of claim 21, wherein the formatter decrypts the information content data, if encrypted.

32. (Original) The system of claim 21, wherein the formatter decrypts the formatting data and the information content data, if encrypted, in response to a valid key.

33. (Original) The system of claim 21, wherein the formatter decrypts each of the formatting data and the information content data, if encrypted, in response to different keys.

34. – 54. (Cancelled)

55. (Currently Amended) A device to process data, comprising:

a formatter to decrypt encrypted formatting data associated with information content data and to format the information content data into a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at each of a plurality of different requesters or clients, and wherein the formatting data is decrypted using a selected key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each of the plurality of different requesters or clients ~~requester or client~~ to provide presentation integrity between each of the plurality of different requesters or clicnts, and wherein the different requesters or clients are involved in a situation together requiring presentation integrity to prevent any confusion, misunderstanding, delays in coordination or other adverse effects between each of the plurality of different requesters or clients involved in the situation; and

an output device to present the information content data in the predetermined format.

56. (Currently Amended) ~~The~~ A device to process data ~~of claim 55~~, ~~wherein the~~ comprising:

a formatter, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter, wherein the information content data is distributable in ~~one form or~~ a single medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver; and

an output devicc to present the information content data in the selected one of thc predetermined formats.

57. (Original) The device of claim 56, wherein each predetermined format provides a different version of the information content data for presentation.

58. (Original) The device of claim 56, wherein the information content data is presentable in different versions of the information content for different audiences, wherein the information content comprises one of a motion picture, an audio, visual or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual or combination audio-visual work.

59. – 72. (Cancelled)

73. (Currently Amended) A method for presentation integrity, comprising:

decrypting encrypted formatting data associated with information content data; and

formatting the associated information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at each of a plurality of different requesters or clients, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each of the plurality of different requesters or clients ~~requester or client~~ to provide presentation integrity between the different rcquesters or clients; and

sending the encrypted formatting data and the information content data to the plurality of clients, wherein the information content data is formatted in the predetermined format at each client, wherein each of the plurality of clients are involved in a single activity requiring presentation integrity to prevent any confusion, misunderstanding, delays in coordination or other adverse effects between each of the plurality of clients.

74. (Cancelled)

75. (Cancelled)

76. (Original) The method of claim 73, wherein the information content data is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the information content data in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

77. (Original) The method of claim 76, further comprising formatting the information content data into different versions for different audiences, wherein the information content data comprises one of an audio, visual, or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual, or combination audio-visual work.

78. (Original) The method of claim 73, wherein the encrypted formatting data is decryptable to format an associated copy of the information content data in the predetermined format in response to a valid key assigned to the associated copy, wherein a different valid key is assigned to each copy of the information content data to only decrypt the formatting data associated with the assigned copy.

79. (Original) The method of claim 73, wherein the encrypted formatting data is decryptable in response to a valid key.

80. (Original) The method of claim 73, further comprising presenting the information content data in the predetermined format to each requestor providing a valid key.

81. (Original) The method of claim 80, wherein presenting the information content data comprises at least one of displaying or printing the information content data in the predetermined format.

82. (Original) The method of claim 73, further comprising decrypting the information content data, if encrypted.

83. (Original) The method of claim 73, wherein the encrypted formatting data and the information content data, if encrypted, are each decryptable in response to a valid key.

84. (Original) The method of claim 73, wherein the encrypted formatting data and the information content data, if encrypted, arc each decryptable in response to a different key.

85. (Original) The method of claim 73, further comprising:

updating the information content data; and

formatting the updated information content data in the predetermined format based on the decrypted formatting data.

86. (Original) The method of claim 73, further comprising encrypting the formatting data into an encrypted style sheet language transformation (SLT).

87. (Original) The method of claim 73, further comprising encrypting the information content data into an encrypted markup language (ML).

88. (Original) The method of claim 73, further comprising transmitting the information content data in an encrypted ML and the formatting data in an encrypted SLT to a requestor.

89. (Original) The method of claim 73, further comprising transmitting the information content data in the predetermined format in hypertext markup language (HTML) to a requestor.

90. – 107. (Cancelled)

108. (Currently Amended) A method to control information content, comprising:

decrypting encrypted formatting data associated with information content data; and formatting the associated information content data in one of a plurality of predetermined formats based on the decrypted formatting data, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, wherein thc information content data is distributable in ~~one~~ a single ~~form or~~ medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

109. (Original) The method of claim 108, further comprising selecting one of the plurality of predetermined formats by decrypting the encrypted formatting data in response to a chosen one of a plurality of keys, each key corresponding to one of the plurality of predetermined formats.

110. (Original) The method of claim 109, further eomprising formatting the information content data in each of the plurality of predetermined formats for a different intended audience.

111. (Original) The method of elaim 108, wherein the information eontent data is one of an audio, visual or eombination audio-visual work.

112. (Original) The method of elaim 108, further eomprising selecting one of a plurality of keys, eaeh key corresponding to one of a plurality of predetermined formats to format the information content data, wherein the encrypted formatting data is decryptable in response to the selected one of the plurality of keys.

113. (Original) The method of claim 108, further comprising decrypting the encrypted formatting data and the information content, if encrypted, in response to a valid key.

114. (Original) The method of claim 108, further comprising decrypting the encrypted formatting data and the information content, if encrypted, in response to different keys.

115.-131. (Cancelled)

132. (Currently Amended) A computer-readable medium encoded with computer-executable instructions for performing a method, comprising:

decrypting encrypted formatting data associated with information content data; and

formatting the associated information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at each of a plurality of different requesters or clients; and

preventing the associated information content data from being presented in the format other than the predetermined format at each of a plurality of requesters or clients ~~requester or client~~ to provide presentation integrity between each of the plurality of ~~the~~ different requesters or clients, wherein the plurality of different requesters or clients are involved in a situation together requiring presentation integrity to prevent any confusion, misunderstanding, delays in coordination or other adverse effects between each of the plurality of different requesters or clients involved in the situation.

133. Canccled

134. (Previously Presented) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 132, further comprising sending thc encrypted formatting data and thc information content data to a plurality of clients, wherein the information content data is formatted in the predetermined format at each client.

135. (Previously Presented) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 132, wherein the information content data is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the

information content data in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

136. (Previously Presented) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 135, further comprising formatting the information content data into different versions for different audiences, wherein the information content data comprises one of an audio, visual, or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual, or combination audio-visual work.

137. (Previously Presented) The computer-readable medium encoded with computer-executable instructions for performing the mcthod of claim 132, wherein the encrypted formatting data is decryptable to format an associated copy of the information content data in the predetermined format in response to a valid key assigned to the associated copy, wherein a different valid key is assigned to each copy of the information content data to only decrypt the formatting data associated with the assigned copy.

138. (Currently Amended) A computer-readable medium encoded with computer-executable instructions for performing a method, comprising:

decrypting encrypted formatting data associated with information content data; and

formatting the associated information content data in one of a plurality of predetermined formats based on the decrypted formatting data, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, wherein the information content data is distributable in ~~one form or~~ a single medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

139. (Previously Presented) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 138, further comprising selecting one of the plurality of predetermined formats by decrypting the encrypted formatting data in response to a chosen one of a plurality of keys, each key corresponding to one of the plurality of predetermined formats.

140. (Previously Presented) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 139, further comprising formatting the information content data in each of the plurality of predetermined formats for a different intended audience.

141. (Previously Presented) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 139, further comprising selecting one of a plurality of keys, each key corresponding to one of a plurality of predetermined formats to format the information content data, wherein the encrypted formatting data is decryptable in response to the selected one of the plurality of keys.